IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Cromer	)	Art Unit: 2152
Serial No.: 09/855,624	)	Examiner: Refai
Filed: May 14, 2001	)	RPS919980030US2
For: AUTOMATIC RECONFIGURATION SYSTEM FOR CHANGE IN MANAGEMENT	)	July 12, 2005 750 B STREET, Suite 3120 San Diego, CA 92101

APPEAL BRIEF

Commissioner of Patents and Trademarks

Dear Sir:

This brief is submitted under 35 U.S.C. §134 and is in accordance with 37 C.F.R. Parts 1, 5, 10, 11, and 41, effective September 13, 2004 and published at 69 Fed. Reg. 155 (August 2004). This brief is further to Appellant's Notice of Appeal filed herewith.

Table of Contents

(1) Real Party in Interest

The real party in interest is Lenovo U.S. Inc.

(2) Related Appeals/Interferences

No other appeals or interferences exist which relate to the present application or appeal.

(3) Status of Claims

Claims 10-15 are pending and finally rejected, which rejections are appealed, and claims 1-9 and 16-20 have been canceled.

(4) Status of Amendments

No amendments are outstanding.

(5) Concise Explanation of Subject Matter in Each Independent Claim, with Page and Figure Nos.

As an initial matter, it is noted that according to the Patent Office, the concise explanations under this section are for Board convenience, and do not supersede what the claims actually state. 69 Fed. Reg. 155 (August 2004), see page 49976. Accordingly, nothing in this Section should be construed as an estoppel that limits the actual claim language.

Claim 10 recites a method for providing update configuration data for a client personal computer system (104, figure 1, page 9, line 3) in a data network including a server having configuration data including an internet protocol destination address. The client personal computer system has a storage device (302, figure 3, page 12, line 7) for storing configuration data and a micro controller (402, figure 4, page 12, line 16) for receiving network signal packets from the server and for configuring the client personal computer system with updated configuration data, including the internet protocol destination address of the server. The method includes receiving a network signal packet sent from the server in the micro controller in the client personal computer system, and determining that the network signal packet includes the server's internet protocol destination address. Also, the method includes determining that the network signal packet is a match for the client personal computer system, and responding to these steps when the packet is a match by updating the storage device of the client personal computer system with the internet protocol destination address of the server.

Claim 15 recites a method for providing update configuration data for a client personal computer system (supra) in a data network including a server. The server has configuration data including an internet protocol destination address, and the network includes at least one client personal computer system (supra) having a storage device for storing configuration data and a micro controller for receiving network signal packets from the server and for configuring the at least one client personal computer system with updated configuration data. The data includes the internet protocol destination address of the server. The method of Claim 15 includes receiving a network signal packet sent from the server in the micro controller in the client personal computer system, and authenticating encryption of the network signal packet to authenticate the presence of encrypted data in the network signal packet. The method further includes validating the data authenticated in the step of authenticating the encryption of the network signal packet, determining that the network signal packet includes the server's internet protocol destination address by determining the presence in the network signal packet of configuration identification and configuration data for the server, and determining that the network signal packet is a match for the any one of the client personal computer system. This last step is done by first determining that the network signal packet is identified to a specific one of the client personal computer systems, and otherwise determining as to whether the network signal packet is identified to a plurality of client personal computer systems. The method also responds to the receiving, determining inclusion of the server's address and determining that the packet is a match by updating the storage device of any identified client personal computer systems with the internet protocol destination address of the server included in the packet.

(6) Grounds of Rejection to be Reviewed on Appeal

(a) Claims 10-13 have been rejected under 35 U.S.C. §102 as being anticipated by Aziz et al., USPN 6,119,234.

(b) Claims 14 and 15 have been rejected under 35 U.S.C. §103 as being unpatentable over Aziz et al. in view of Crowle, USPN 5,857,072.

(7) Argument

As an initial matter, it is noted that according to the Patent Office, a new ground of rejection in an examiner's answer should be "rare", and should be levied only in response to such things as newly presented arguments by Applicant or to address a claim that the examiner previously failed to address, 69 Fed. Reg. 155 (August 2004), see, e.g., pages 49963 and 49980. Furthermore, a new ground of rejection must be approved by the Technology Center Director or designee and in any case must come accompanied with the initials of the conferees of the appeal conference, id., page 49979.

(a) This appeal has been made necessary because the examiner refuses to recognize right answer when told, and since the SPE signed out the last office action, this is particularly discouraging. Specifically, the SPE who signed out the office action continues to allege that Aziz et al., col. 2, lines 52-58 teach receiving a packet from a server at a client, when in fact this section mentions nothing about packets much less storing a server packet at a client but instead merely teaches that the addresses of authorized clients can be stored at a host for selectively establishing client access to protected hosts, just as Appellant's last response said. Nevertheless, the SPE who signed out the Office Action stubbornly insists that because packets are well known, the relied-upon section of Aziz et al. therefore inherently teaches it, a plain logical *non-sequitur* (to be inherent, an element must necessarily be part of a reference, MPEP §2112, and there is no question that communication can occur without packets). For this reason alone, the rejections under this section are overcome. Because the SPE has vetted the last response, it would be highly inappropriate for him to authorize reopening prosecution and thus short-circuiting the appellate process, because neither the issue nor Appellant's response, which the SPE has signed off as considering and rejecting, have materially changed.

Continuing, the rejections continue to allege that Aziz et al., col. 3, lines 38-50 teach determining that the packet contains the server's IP address, when in fact this section simply teaches that to allow a client to penetrate a firewall, the client needs the address of the firewall, which has not been relied on as the claimed server, and not the address of the server itself. Even if the firewall is taken to be the claimed server, there is no determination of anything, much less the contents of a packet, taught in the relied-on section. The SPE responds to this exposition by alleging another *non-sequitur*, namely, that Aziz et al. teaches that an administrator stores host addresses. But that is not what is being claimed. It is noteworthy that the SPE studiously ignores mention of where, precisely, Aziz et al. discusses "determining" anything.

The SPE disagrees with Appellant that Aziz et al. fails to disclose matching a packet with a client, responding that the relied-upon sections of Aziz et al. "would need" to perform the untaught step. However, there is no "need" for packet matching in a discussion that nowhere mentions packets but instead focuses on secure communication and authentication, and component configuration. Essentially, the SPE admits that the claimed feature is not taught in the applied reference but insists that the claim cannot be novel anyway because, in the SPE's unsupported opinion, the reference "needs" to have it.

Perhaps most damning of the SPE's case is the allegation that because updating a configuration file is taught in Aziz et al. at col. 2, lines 50-67, then the last element of Claim 10 is also taught. Nothing is more unhinged from reality, however. Only the present invention of Claim 10 updates the storage device of the client with the IP destination address of the server that is included in the packet when a match is determined. Aziz et al. says nothing about updating a configuration file using a packet, much less using a specific piece of information in the packet, much less still based on the explicitly recited test outcome of Claim 10. The rejections under this section are overcome.

(b) Many of the same errors propagate through to the obviousness rejections. Additionally, the SPE contradicts himself by admitting here that Aziz et al. fails to perform the claimed match, despite alleging the opposite in the anticipation rejection. Appellant agrees with the examiner that Aziz et al. fails to teach the claimed match, and disagrees that Crowle can be used to fill the gap for the following reasons. Claim 15 requires one element (authenticating encryption of the network signal packet to authenticate the presence of encrypted data in the network signal packet) that is alleged to be taught in Aziz et al., but is not, and no citation to Aziz et al. accompanies the allegation. Further, Claim 15 recites validating the authenticated data, but no mention is made of this element in the rejection. The SPE, having had an opportunity twice to properly consider these limitations, should either allow the claim or pass the application on to the Board, but should not in fairness reopen prosecution. Should the SPE wish to lodge a new ground of rejection the appropriate course would be to do so in the context of a new ground of rejection in his Answer, so that the course of prosecution will be brought to the attention of the Group Director, who must approve of new grounds in an Answer.

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

APPENDIX A - APPEALED CLAIMS

10. A method for providing update configuration data for a client personal computer system in a data network including a server, having configuration data including an internet protocol destination address, and at least one client personal computer system having a storage device for storing configuration data and a micro controller for receiving network signal packets from the server and for configuring the client personal computer system with updated configuration data, including the internet protocol destination address of the server, comprising the steps of:

receiving a network signal packet sent from the server in the micro controller in the at least one client personal computer system;

determining that the network signal packet includes the server's internet protocol destination address;

determining that the network signal packet is a match for the any one of the at least one client personal computer system; and

responding to the receiving, determining inclusion of the server's address and determining that the packet is a match by updating the storage device of the any one of the at least one client personal computer system with the included internet protocol destination address of the server included in the packet.

11. The method as defined in Claim 10, wherein, after the step of receiving the network signal packet, there is a step of authenticating the encryption of the network signal packet to authenticate the presence of encrypted data in the network signal packet.

12. The method as defined in Claim 11, wherein, after the step of authenticating the encryption of the network packet, there is a step of validation of the data authenticated in the step of authenticating the encryption of the network packet.

13. The method as defined in Claim 12, wherein in determining that the network signal packet includes the server's internet protocol destination address, the presence in the network signal packet of configuration identification and configuration data is determined.

14. The method as defined in Claim 13, wherein in the step of determining whether the network signal packet is a match for any one of the at least one client personal computer system, there is a first determination as to whether the network signal packet is identified to any one of the least one client personal computer systems and a second determination as to whether the network signal packet is identified to a plurality of client personal computer systems.

15. A method for providing update configuration data for a client personal computer system in a data network including a server, having configuration data including an internet protocol destination address, and at least one client personal computer system having a storage device for storing configuration data and a micro controller for receiving network signal packets from the server and for configuring the at least one client

personal computer system with updated configuration data, including the internet protocol destination address of the server, comprising the steps of:

receiving a network signal packet sent from the server in the micro controller in the at least one client personal computer system;

authenticating encryption of the network signal packet to authenticate the presence of encrypted data in the network signal packet;

validating the data authenticated in the step of authenticating the encryption of the network signal packet;

determining that the network signal packet includes the server's internet protocol destination address by determining the presence in the network signal packet of configuration identification and configuration data for the server;

determining that the network signal packet is a match for the any one of the at least one client personal computer systems by first determining that the network signal packet is identified to a specific one of the at least one client personal computer systems and otherwise determining as to whether the network signal packet is identified to a plurality of client personal computer systems; and

responding to the receiving, determining inclusion of the server's address and determining that the packet is a match by updating the storage device of any identified client personal computer systems with the internet protocol destination address of the server included in the packet.

APPENDIX B - EVIDENCE

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)

APPENDIX C - RELATED PROCEEDINGS

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)